

Constacyclic codes over

$$\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q^*$$

Joël Kaboré and Mohammed E. Charkani

Department of Mathematics, Faculty of Sciences
Dhar-Mahraz-Fès, Sidi Mohamed Ben Abdellah University

E-mail: jokabore@yahoo.fr

Department of Mathematics, Faculty of Sciences
Dhar-Mahraz-Fès, Sidi Mohamed Ben Abdellah University

E-mail: mcharkani@gmail.com

Abstract

Let q be a prime power and \mathbb{F}_q be a finite field. In this paper, we study constacyclic codes over the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v$ and $uv = vu$. We characterize the generator polynomials of constacyclic codes and their duals using some decomposition of this ring. Finally we study the images of self-dual cyclic codes over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ through a linear Gray map.

Keywords: Constacyclic code, generator polynomial, self-dual code, Gray map.

1 Introduction

Constacyclic codes are an important class of linear block codes. These codes possess rich algebraic structures and can be efficiently encoded using shift registers. It's well-known that for a given unit λ , λ -constacyclic codes over a ring R are ideals of the ring $R[x]/\langle x^n - \lambda \rangle$. The last years, these kinds of code have been studied over many classes of finite chain rings [6, 3, 11, 8, 5]. Recently, other classes of rings which are non-chain rings have been introduced. Linear codes and some constacyclic codes over some local Frobenius ring have been studied [7, 12]. Most recently constacyclic codes over finite principal ideal ring have been investigated [2]. Some results on linear and cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ established in [16] have been extended in [4] to the ring $\mathbb{F}_2[u_1, u_2, \dots, u_k]/\langle u_i^2 - u_i, u_i u_j - u_j u_i \rangle$. The ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu$ has been used as alphabet to study linear codes and skew-cyclic codes [14]. In the same way, we generalize some results of [15] on constacyclic codes over $\mathbb{F}_q + v\mathbb{F}_q, v^2 = v$ to the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu$.

This paper is organized as follows. In section 2, we give some properties of the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, and investigate some results about constacyclic codes. In section 3, we characterize the generator polynomials of constacyclic codes, their duals and self-dual constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. In section 4, we define a Gray map over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, and characterize the Gray images of self-dual cyclic codes.

2 Preliminaries

Let R be denote the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v$ and \mathbb{F}_q be a finite field with q elements, q is a power of a prime p . This ring is a finite commutative ring with characteristic p and it contains four maximal ideals which are:

$$\mathfrak{m}_1 = \langle u, v \rangle, \mathfrak{m}_2 = \langle u - 1, v - 1 \rangle, \mathfrak{m}_3 = \langle u - 1, v \rangle, \mathfrak{m}_4 = \langle u, v - 1 \rangle.$$

These ideals have 1 as index of stability. Let

$$\varphi : R \rightarrow R/\mathfrak{m}_1 \times R/\mathfrak{m}_2 \times R/\mathfrak{m}_3 \times R/\mathfrak{m}_4 \quad (\cong \mathbb{F}_q^4),$$

be the canonical homomorphism defined by $x \mapsto (x + \mathfrak{m}_1, x + \mathfrak{m}_2, x + \mathfrak{m}_3, x + \mathfrak{m}_4)$. By the ring version of the Chinese Remainder Theorem, the map φ is an isomorphism; from this we see that R is a principal ideal ring.

We recall a fundamental result on the decomposition of modules.

Lemma 2.1 ([1], Proposition 7.2)

Let R be a finite ring and I_1, I_2, \dots, I_n be ideals of R . The following statements are equivalent about the R -module R :

- i) $R = I_1 \oplus I_2 \oplus \dots \oplus I_n$;
- ii) *There exists a unique family $(e_i)_{i=1}^n$ of idempotents of R such that $e_i e_j = 0$ for $i \neq j$, $1 = \sum_{i=1}^n e_i$ and $I_i = Re_i$.*

Let $e_1 = 1 - u - v + uv, e_2 = uv, e_3 = u - uv, e_4 = v - uv$. It is easy to verify that $e_i^2 = e_i, e_i e_j = 0$ and $1 = \sum_{k=1}^4 e_k$, with $i, j = 1, 2, 3, 4, i \neq j$ and $Re_i \cong \mathbb{F}_q$. We deduce, from previous lemma that: $R = Re_1 \oplus Re_2 \oplus Re_3 \oplus Re_4$. Any element of R can be expressed as: $r = a + bu + cv + duv = e_1 a + e_2(a + b + c + d) + e_3(a + b) + e_4(a + c)$, with $a, b, c, d \in \mathbb{F}_q$. Let :

$$\begin{aligned} \varphi : \quad R &\longrightarrow \mathbb{F}_q^4 \\ r = a + bu + cv + duv &\longmapsto (\varphi_1(r), \varphi_2(r), \varphi_3(r), \varphi_4(r)) \end{aligned}$$

Where

$$\begin{aligned} \varphi_1 : \quad R &\longrightarrow R/\mathfrak{m}_1 \cong \mathbb{F}_q \\ r = a + bu + cv + duv &\longmapsto a. \end{aligned}$$

$$\begin{aligned} \varphi_2 : \quad R &\longrightarrow R/\mathfrak{m}_2 \cong \mathbb{F}_q \\ r = a + bu + cv + duv &\longmapsto a + b + c + d. \end{aligned}$$

$$\begin{aligned} \varphi_3 : \quad R &\longrightarrow R/\mathfrak{m}_3 \cong \mathbb{F}_q \\ r = a + bu + cv + duv &\longmapsto a + b. \end{aligned}$$

$$\begin{aligned} \varphi_4 : \quad R &\longrightarrow R/\mathfrak{m}_4 \cong \mathbb{F}_q \\ r = a + bu + cv + duv &\longmapsto a + c. \end{aligned}$$

By the module version of chinese remainder theorem, φ is an R -module isomorphism. This map can be extended to R^n . For a code $\mathcal{C} \subseteq R^n$, we denote $\varphi_i(\mathcal{C})$ by \mathcal{C}_i

for $1 \leq i \leq 4$; then we have $\mathcal{C} \cong \mathcal{C}_1 \times \mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_4$ and $|\mathcal{C}| = |\mathcal{C}_1||\mathcal{C}_2||\mathcal{C}_3||\mathcal{C}_4|$. Note that an element $\lambda = a + bu + cv + duv \in R^*$ is a unit if and only if $\forall i \in \{1, 2, 3, 4\}, \varphi_i(\lambda)$ is a unit in \mathbb{F}_q if and only if $a \neq 0, a + b + c + d \neq 0, a + b \neq 0$ and $a + c \neq 0$.

The following result is a consequence of theorem 4.9 of [2].

Lemma 2.2 *Let $\lambda = a + bu + cv + duv$ be a unit in R and $\mathcal{C} = \varphi^{-1}(\mathcal{C}_1 \times \mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_4)$ be a code of length n over R . Then \mathcal{C} is a λ -constacyclic code over R if and only if $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$ are a -constacyclic, $(a + b + c + d)$ -constacyclic, $(a + b)$ -constacyclic, and $(a + c)$ -constacyclic codes of length n over \mathbb{F}_q , respectively.*

3 Constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ *

Now we investigate constacyclic codes over R . From the previous section, we know that any code over R can be uniquely expressed as $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$. Let $\lambda = a + bu + cv + duv$ be a unit in R . We let $\lambda_1 = a, \lambda_2 = a + b + c + d, \lambda_3 = a + b$ and $\lambda_4 = a + c$.

Theorem 3.1 *Let $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$ be a λ -constacyclic code of length n over R . Then $\mathcal{C} = \langle e_1g_1(x), e_2g_2(x), e_3g_3(x), e_4g_4(x) \rangle$, where $g_i(x)$ is a generator polynomial of λ_i -constacyclic code $\mathcal{C}_i, 1 \leq i \leq 4$. Furthermore $|\mathcal{C}| = q^{4n - \sum_{i=1}^4 \deg g_i(x)}$.*

Proof. If $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$ is a λ -constacyclic code of length n over R , then from lemma 2.2, \mathcal{C}_i is a λ_i -constacyclic code of length n over \mathbb{F}_q . So there exists polynomials $g_1(x), g_2(x), g_3(x), g_4(x)$ such that $\mathcal{C}_i = \langle g_i(x) \rangle$, for $1 \leq i \leq 4$. Let $r(x) \in \mathcal{C}$, since $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$, then there exists $f_i(x) \in \mathcal{C}_i = \langle g_i(x) \rangle, 1 \leq i \leq 4$ such that $r(x) = \sum_{i=1}^4 e_i f_i(x)$, i.e. there exists $h_i(x) \in \mathbb{F}_q[x]$ such that $r(x) = \sum_{i=1}^4 e_i h_i(x) g_i(x)$. Hence $r(x) \in \langle e_1g_1(x), e_2g_2(x), e_3g_3(x), e_4g_4(x) \rangle$ i.e. $\mathcal{C} \subseteq \langle e_1g_1(x), e_2g_2(x), e_3g_3(x), e_4g_4(x) \rangle$.

Reciprocally if $r(x) \in \langle e_1g_1(x), e_2g_2(x), e_3g_3(x), e_4g_4(x) \rangle$, there are polynomials $k_i(x) \in R[x]/\langle x^n - \lambda \rangle$ such that $r(x) = \sum_{i=1}^4 e_i g_i(x) k_i(x)$; then there are $r_i(x) \in \mathbb{F}_q[x]$ such that $r(x) = \sum_{i=1}^4 e_i g_i(x) r_i(x)$ where $g_i(x) r_i(x) \in \mathcal{C}_i \subseteq \mathbb{F}_q[x]/\langle x^n - \lambda_i \rangle$; therefore $r(x) \in \mathcal{C}$ and $\langle e_1g_1(x), e_2g_2(x), e_3g_3(x), e_4g_4(x) \rangle \subseteq \mathcal{C}$; which implies that $\mathcal{C} = \langle e_1g_1(x), e_2g_2(x), e_3g_3(x), e_4g_4(x) \rangle$.

Since $|\mathcal{C}| = |\mathcal{C}_1||\mathcal{C}_2||\mathcal{C}_3||\mathcal{C}_4|$, we deduce that $|\mathcal{C}| = q^{4n - \sum_{i=1}^4 \deg g_i(x)}$. \square

For any code of length n over R and any $r \in R$, we denote by $(\mathcal{C} : r)$ the submodule quotient defined as follows:

$$(\mathcal{C} : r) = \{s \in R^n | rs \in \mathcal{C}\}.$$

Lemma 3.2 *Let $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$ be a linear code over R . Then:*

$$\varphi_i((\mathcal{C} : e_i)) = \mathcal{C}_i, \forall 1 \leq i \leq 4.$$

Proof. Let $r \in (\mathcal{C} : e_i)$, then $e_i r \in \mathcal{C}$. We can write r as: $r = e_1 \varphi_1(r) + e_2 \varphi_2(r) + e_3 \varphi_3(r) + e_4 \varphi_4(r)$; then $e_i r = e_i \varphi_i(r)$, $1 \leq i \leq 4$, which implies that $\varphi_i(r) \in \mathcal{C}_i$, $1 \leq i \leq 4$ hence $\varphi_i((\mathcal{C} : e_i)) \subseteq \mathcal{C}_i$, $1 \leq i \leq 4$.

Reciprocally, for any $r_1 \in \mathcal{C}_1$ there exists $r_2, r_3, r_4 \in \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$, respectively such that: $e_1 r_1 + e_2 r_2 + e_3 r_3 + e_4 r_4 \in \mathcal{C}$. We see that $e_1 r_1 = e_1(e_1 r_1 + e_2 r_2 + e_3 r_3 + e_4 r_4) \in e_1 \mathcal{C} \subseteq \mathcal{C}$ and $r_1 = e_1 r_1 + e_2 r_1 + e_3 r_1 + e_4 r_1$; so $r_1 \in (\mathcal{C} : e_1)$ and $\varphi_1(r_1) = r_1$. Then $r_1 \in \varphi_1((\mathcal{C} : e_1))$, hence $\mathcal{C}_1 \subseteq \varphi((\mathcal{C} : e_1))$. The proof is the same for the other cases. \square

The following result is a generalization of theorem 3.5 in [15].

Theorem 3.3 *Let $\mathcal{C} = e_1 \mathcal{C}_1 \oplus e_2 \mathcal{C}_2 \oplus e_3 \mathcal{C}_3 \oplus e_4 \mathcal{C}_4$ be a λ -constacyclic code of length n over R . We suppose that $\mathcal{C} = \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x), e_4 g_4(x) \rangle$, where polynomials $g_i(x)$, $1 \leq i \leq 4$ are monic with $g_i(x)$ divides $(x^n - \lambda_i)$ for $1 \leq i \leq 4$. Then, for $1 \leq i \leq 4$, $g_i(x)$ is the generator polynomial of λ_i -constacyclic code.*

Proof. For a polynomial $f(x) \in (\mathcal{C} : e_i)$, we have $e_i f(x) \in \mathcal{C}$. Since $\mathcal{C} = \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x), e_4 g_4(x) \rangle$, then for $1 \leq j \leq 4$, there exists $s_j(x) \in R[x] / \langle x^n - \lambda \rangle$ such that $e_i f(x) = \sum_{j=1}^4 e_j g_j(x) s_j(x)$. Furthermore $f(x) = \sum_{i=1}^4 e_i \varphi_i(f(x))$ and $s_j(x) = \sum_{j=1}^4 e_j \varphi_j(s_j(x))$; hence

$$e_i \left[\sum_{j=1}^4 e_j \varphi_j(f(x)) \right] = \sum_{j=1}^4 e_j g_j(x) \left[\sum_{j=1}^4 e_j \varphi_j(s_j(x)) \right].$$

This implies that $e_i \varphi_i(f(x)) = \sum_{j=1}^4 e_j g_j(x) \varphi_j(s_j(x))$. We deduce: $\varphi_i(f(x)) = g_i(x) \varphi_i(s_i(x))$. So $\varphi_i(f(x)) \in \langle g_i(x) \rangle$. Reciprocally, if $f(x) \in \langle g_i(x) \rangle$, then there exists $r(x) \in \mathbb{F}_q$ such that $f(x) = g_i(x) r(x)$. This implies that $e_i f(x) = e_i g_i(x) r(x) \in \mathcal{C}$, i.e. $f(x) \in (\mathcal{C} : e_i)$. Since $f(x) = \sum_{i=1}^4 e_i f(x)$, then $\varphi_i(f(x)) = f(x)$, hence $f(x) \in \varphi_i((\mathcal{C} : e_i))$. This implies that $\langle g_i(x) \rangle \subseteq \varphi_i((\mathcal{C} : e_i))$. The result follows from lemma 3.2. \square

Theorem 3.4 *Let \mathcal{C} be a λ -constacyclic code over R and $g_i(x)$ be the monic generator polynomial of the code \mathcal{C}_i , $1 \leq i \leq 4$. Then there exists a unique polynomial $g(x) \in R[x]$ such that $\mathcal{C} = \langle g(x) \rangle$ and $g(x)$ is a divisor of $x^n - \lambda$.*

Proof.

◦ Let $g(x) = \sum_{i=1}^4 e_i g_i(x)$. It's obvious that $\langle g(x) \rangle \subseteq \mathcal{C}$. Reciprocally, it's clear that $e_i g_i(x) = e_i (\sum_{j=1}^4 e_j g_j(x)) = e_i g(x)$, $\forall 1 \leq i \leq 4$, which implies that $\mathcal{C} \subseteq \langle g(x) \rangle$, hence $\mathcal{C} = \langle g(x) \rangle$.

◦ Unicity of $g(x)$: we suppose that there exists another polynomial $h(x)$ in $R[x] / \langle x^n - \lambda \rangle$ such that $\mathcal{C} = \langle h(x) \rangle$. For $1 \leq i \leq 4$, we have $e_i h(x) = e_i [\sum_{j=1}^4 e_j \varphi_j(h(x))] = e_i \varphi_i(h(x)) \in \mathcal{C}$. This implies $\varphi_i(h(x)) \in \varphi_i((\mathcal{C} : e_i)) = \mathcal{C}_i$ (from lemma 3.2). Since $\mathcal{C}_i = \langle g_i(x) \rangle$, we deduce that $g_i(x)$ divides $\varphi_i(h(x))$, $1 \leq i \leq 4$. Conversely, since $\langle g(x) \rangle = \langle h(x) \rangle$, there exists polynomial $k(x) \in R[x] / \langle x^n - \lambda \rangle$ such that:

$$\sum_{i=1}^4 e_i g_i(x) = k(x) h(x) = \left[\sum_{j=1}^4 e_j \varphi_j(k(x)) \right] \left[\sum_{j=1}^4 e_j \varphi_j(h(x)) \right] = \sum_{j=1}^4 e_j \varphi_j(k(x)) \varphi_j(h(x)).$$

It follows that $g_i(x) = \varphi_i(k(x))\varphi_i(h(x))$ i.e. $\varphi_i(h(x))$ divides $g_i(x), \forall 1 \leq i \leq 4$. Then we conclude that $\varphi_i(h(x)) = g_i(x), \forall 1 \leq i \leq 4$; so $h(x) = g(x)$ in $R[x]/\langle x^n - \lambda \rangle$.

◦ Now we show that the polynomial $g(x) \in R[x]/\langle x^n - \lambda \rangle$ is a divisor of $x^n - \lambda$. We know that $g(x) = \sum_{i=1}^4 e_i g_i(x)$, where $g_i(x)$ is monic generator polynomial of λ_i -constacyclic code $\mathcal{C}_i, 1 \leq i \leq 4$. Then $g_i(x)$ is a divisor of $x^n - \lambda_i$ in $\mathbb{F}_q[x]$. This implies that there exists $h_i(x) \in \mathbb{F}_q[x]$ such that $x^n - \lambda_i = g_i(x)h_i(x)$. Thus $(\sum_{j=1}^4 e_j g_j(x))(\sum_{j=1}^4 e_j h_j(x)) = \sum_{j=1}^4 e_j g_j(x)h_j(x) = \sum_{j=1}^4 e_j(x^n - \lambda_j) = \sum_{j=1}^4 e_j \varphi_j(x^n - \lambda) = x^n - \lambda$. Therefore $g(x)$ divides $x^n - \lambda$. \square

As a consequence of previous theorem we have:

Corollary 3.5 *Let λ be an unit in R ; $\frac{R[x]}{\langle x^n - \lambda \rangle}$ is a principal ideal ring.*

Now we discuss about dual of constacyclic codes over R . Given codewords $r = (r_0, r_1, \dots, r_{n-1})$, $s = (s_0, s_1, \dots, s_{n-1}) \in R^n$, their inner product is defined in the usual way:

$$r.s = r_0 s_0 + r_1 s_1 + \dots + r_{n-1} s_{n-1}, \text{ evaluated in } R.$$

The dual code \mathcal{C}^\perp of \mathcal{C} is the set of n -tuples over R that are orthogonal to all codewords of \mathcal{C} , i.e.:

$$\mathcal{C}^\perp = \{r | r.s = 0, \forall s \in \mathcal{C}\}.$$

The code \mathcal{C} is called self-dual if $\mathcal{C} = \mathcal{C}^\perp$.

It's well-known that for linear codes of length n over a finite frobenius ring R , $|\mathcal{C}||\mathcal{C}^\perp| = |R|^n$ ([13]). For a given unit $\lambda \in R$, the dual of λ -constacyclic code over R is a λ^{-1} -constacyclic code ([6, 11]). Let $f(x)$ be the polynomial $f(x) = a_0 + a_1 x + \dots + a_r x^r \in R[x]$, and i be the smallest integer such that $a_i \neq 0$. The reciprocal polynomial of f denoted by f^* is defined as $f^*(x) = x^{r+i} f(x^{-1}) = a_r x^i + a_{r-1} x^{i+1} + \dots + a_i x^r$. The following result characterizes the dual of a λ -constacyclic code over R .

Theorem 3.6 *Let $\mathcal{C} = e_1 \mathcal{C}_1 \oplus e_2 \mathcal{C}_2 \oplus e_3 \mathcal{C}_3 \oplus e_4 \mathcal{C}_4$ be a λ -constacyclic code of length n over R , such that $\mathcal{C} = \langle e_1 g_1(x), e_2 g_2(x), e_3 g_3(x), e_4 g_4(x) \rangle$ and \mathcal{C}^\perp its dual. Let $h_i(x) \in \mathbb{F}_q[x]$ such that $g_i(x)h_i(x) = x^n - \lambda_i$. Then $\mathcal{C}^\perp = e_1 \mathcal{C}_1^\perp \oplus e_2 \mathcal{C}_2^\perp \oplus e_3 \mathcal{C}_3^\perp \oplus e_4 \mathcal{C}_4^\perp$, where \mathcal{C}_i^\perp is the dual of the λ_i -constacyclic code over \mathbb{F}_q . Furthermore $\mathcal{C}^\perp = \langle e_1 h_1^*(x) + e_2 h_2^*(x) + e_3 h_3^*(x) + e_4 h_4^*(x) \rangle$.*

Proof. Let $s_i \in \mathcal{C}_i^\perp, 1 \leq i \leq 4$ and $r = \sum_{i=1}^4 e_i r_i \in \mathcal{C}$ with $r_i \in \mathcal{C}_i, 1 \leq i \leq 4$. We have that: $r.(\sum_{i=1}^4 e_i s_i) = (\sum_{i=1}^4 e_i r_i)(\sum_{i=1}^4 e_i s_i) = \sum_{i=1}^4 e_i r_i s_i = 0$. This implies that $e_1 \mathcal{C}_1^\perp \oplus e_2 \mathcal{C}_2^\perp \oplus e_3 \mathcal{C}_3^\perp \oplus e_4 \mathcal{C}_4^\perp \subseteq \mathcal{C}^\perp$. Note that $|e_1 \mathcal{C}_1^\perp \oplus e_2 \mathcal{C}_2^\perp \oplus e_3 \mathcal{C}_3^\perp \oplus e_4 \mathcal{C}_4^\perp| = |\mathcal{C}_1^\perp| |\mathcal{C}_2^\perp| |\mathcal{C}_3^\perp| |\mathcal{C}_4^\perp|$. Since R is a finite frobenius ring, then $|\mathcal{C}||\mathcal{C}^\perp| = |R|^n$. So :

$$\begin{aligned} |\mathcal{C}^\perp| &= \frac{|R|^n}{|\mathcal{C}|} = \frac{q^{4n}}{q^{4n - \sum_{i=1}^4 \deg g_i(x)}} = q^{\sum_{i=1}^4 \deg g_i(x)} \\ &= |e_1 \mathcal{C}_1^\perp \oplus e_2 \mathcal{C}_2^\perp \oplus e_3 \mathcal{C}_3^\perp \oplus e_4 \mathcal{C}_4^\perp|. \end{aligned}$$

Hence $\mathcal{C}^\perp = e_1 \mathcal{C}_1^\perp \oplus e_2 \mathcal{C}_2^\perp \oplus e_3 \mathcal{C}_3^\perp \oplus e_4 \mathcal{C}_4^\perp$.

Let $h_i(x) \in \mathbb{F}_q[x]$ such that $g_i(x)h_i(x) = x^n - \lambda_i$. Since \mathcal{C}_i is a λ_i -constacyclic code of length n over \mathbb{F}_q , with generator polynomial $g_i(x)$, then \mathcal{C}_i^\perp is a λ_i^{-1} -constacyclic code with generator polynomial $h_i^*(x)$ that we can suppose monic. From theorem 3.1 and theorem 3.4, we conclude that $\mathcal{C}^\perp = \langle e_1 h_1^*(x) + e_2 h_2^*(x) + e_3 h_3^*(x) + e_4 h_4^*(x) \rangle$. \square

It's well-known that a λ -constacyclic code over a finite field can be self-dual if and only if $\lambda^2 = 1$. So the only self-dual constacyclic codes over finite fields are cyclic and negacyclic codes. Then \mathcal{C} is self-dual code over R if and only if each \mathcal{C}_i is a self-dual cyclic or negacyclic code over \mathbb{F}_q if and only if $g_i(x)$ and $h_i^*(x)$ are associate in $\mathbb{F}_q[X]$, where $h_i(x)g_i(x) = x^n - \lambda_i$ in $\mathbb{F}_q[x]$, with $\lambda_i = \pm 1$.

4 Gray map with applications

We define a gray map $\phi_1 : R \longrightarrow \mathbb{F}_q^4$ by

$$\phi_1(a + bu + cv + duv) = (d, c + d, b + d, a + b + c + d).$$

This map can be extended to R^n in a natural way:

$$\begin{aligned} \phi : R^n &\longrightarrow \mathbb{F}_q^{4n} \\ (r_0, r_1, \dots, r_{n-1}) &\longmapsto (\phi_1(r_1), \phi_1(r_2), \dots, \phi_1(r_{n-1})). \end{aligned}$$

For any element $a + bu + cv + duv \in R$, we define the Lee weight, denoted by W_L , as $W_L(a + ub + cv + duv) = W_H(d, c + d, b + d, a + b + c + d)$, where W_H denotes the ordinary Hamming weight for q -ary codes. The Lee weight of a codeword $r = (r_1, r_2, \dots, r_{n-1}) \in R^n$ is defined as $W_L(r) = \sum_{i=1}^{n-1} W_L(r_i)$ and for $r, r' \in R^n$, the Lee distance is defined as $d_L(r, r') = W_L(r - r')$. The minimum Lee distance is defined as $\min\{d_L(r, r') \mid r, r' \in \mathcal{C}, r \neq r'\}$. We denote the Hamming distance of a q -ary code \mathcal{C} by $d_H(\mathcal{C})$. The following two results are obvious.

Proposition 4.1 *The Gray map ϕ is a \mathbb{F}_q -linear distance-preserving map from $(R^n, \text{Lee distance})$ to $(\mathbb{F}_q^{4n}, \text{Hamming distance})$.*

Lemma 4.2 *Let $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$ be a linear code of length n over R , size q^k and minimum Lee distance d_L , then $\phi(\mathcal{C})$ is a $[4n, k, d_L]$ -linear code over \mathbb{F}_q .*

Theorem 4.3 *Let $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$ be a linear code of length n over R . Then*

$$d_L(\mathcal{C}) = \min\{d_H(\mathcal{C}_1), 4d_H(\mathcal{C}_2), 2d_H(\mathcal{C}_3), 2d_H(\mathcal{C}_4)\}.$$

Proof. The result is obvious because for any codeword $r \in \mathcal{C}$, we have:

$$\phi(r) = \phi(e_1r_1 + e_2r_2 + e_3r_3 + e_4r_4) = (r_1 + r_2 - r_3 - r_4, r_2 - r_3, r_2 - r_4, r_2),$$

where $r_1 \in \mathcal{C}_1, r_2 \in \mathcal{C}_2, r_3 \in \mathcal{C}_3, r_4 \in \mathcal{C}_4$. \square

Let σ be the cyclic shift on R^n defined by $\sigma(r_0, r_1, \dots, r_{n-1}) = (r_{n-1}, \dots, r_{n-2})$ and $n = n'l$. A linear code which is invariant under σ^l is called a l -quasi-cyclic code of length n .

Theorem 4.4 *A linear code \mathcal{C} of length n over R is a cyclic code if and only if $\phi(\mathcal{C})$ is a 4- quasi-cyclic code of length $4n$ over \mathbb{F}_q .*

Proof. Let $r = (r'_0, r'_1, \dots, r'_{n-1}) \in R^n$, where $r'_i = a_i + b_i u + c_i v + d_i uv$ with $a_i, b_i, c_i, d_i \in \mathbb{F}_q, 0 \leq i \leq n-1$. A simple calculation shows that :

$$\phi(\sigma(r)) = \sigma^4(\phi(r)).$$

Then if \mathcal{C} is a cyclic code of length n over R , we have:

$$\sigma^4(\phi(\mathcal{C})) = \phi(\sigma(\mathcal{C})) = \phi(\mathcal{C}).$$

This implies that $\phi(\mathcal{C})$ is 4- quasi cyclic code of length $4n$ over \mathbb{F}_q .

The other case is obvious because ϕ is an injection. \square

From [10, 9], we know that there exists self-dual cyclic codes of length n over a finite field \mathbb{F}_q if and only if n is even and q is a power of 2.

Theorem 4.5 *Let $\mathcal{C} = e_1\mathcal{C}_1 \oplus e_2\mathcal{C}_2 \oplus e_3\mathcal{C}_3 \oplus e_4\mathcal{C}_4$ be a self-dual cyclic code over $R_2 = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$. Then $\phi(\mathcal{C})$ is a self-dual 4- quasi-cyclic code over \mathbb{F}_{2^m} .*

Proof. If $r_1, r_2 \in \mathcal{C}$, then they can be written as follows:

$r_1 = e_1a_1g_1 + e_2a_2g_2 + e_3a_3g_3 + e_4a_4g_4; r_2 = e_1b_1g_1 + e_2b_2g_2 + e_3b_3g_3 + e_4b_4g_4$; where $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in R_2$ and g_1, g_2, g_3, g_4 are generator polynomials of $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$, respectively. If \mathcal{C} is self-dual code over R_2 , then each \mathcal{C}_i is self-dual cyclic code over \mathbb{F}_{2^m} , so $g_i^2 = 0$ in $\mathbb{F}_{2^m}[x]/\langle x^n - 1 \rangle$ and also in $R_2[x]/\langle x^n - 1 \rangle$. Using this fact and because R_2 has characteristic 2, we easily check that: $\phi(r_1) \cdot \phi(r_2) = 0$; where

$\phi(r_1) = (a_1g_1 + a_2g_2 - a_3g_3 - a_4g_4, a_2g_2 - a_3g_3, a_2g_2 - a_4g_4, a_2g_2)$ and

$\phi(r_2) = (b_1g_1 + b_2g_2 - b_3g_3 - b_4g_4, b_2g_2 - b_3g_3, b_2g_2 - b_4g_4, b_2g_2)$. \square

Now, we give some examples of self-dual cyclic codes over R_2 and their Gray images to illustrate the above results.

Example 4.6 *A self-dual cyclic code of length 14 over $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. The factorisation of $x^{14} + 1$ over \mathbb{F}_2 is given by:*

$$x^{14} + 1 = (x + 1)^2(x^3 + x + 1)^2(x^3 + x^2 + 1)^2.$$

Let \mathcal{C} be the cyclic code over R_2 generated by: $g(x) = e_1g_1(x) + e_2g_2(x) + e_3g_3(x) + e_4g_4(x)$, where $g_1(x) = g_3(x) = x^7 + x^6 + x^3 + x^2 + x + 1, g_2(x) = x^7 + 1$ and $g_4(x) = x^7 + x^6 + x^5 + x^4 + x + 1$. The codes $\mathcal{C}_1 = \mathcal{C}_3 = g_1(x)\mathbb{F}_2[x]$ are $[14, 7, 4]$ self-dual cyclic, $\mathcal{C}_2 = g_2(x)\mathbb{F}_2[x]$ is $[14, 7, 2]$ self-dual cyclic and $\mathcal{C}_4 = g_4(x)\mathbb{F}_2[x]$ is $[14, 7, 4]$ self-dual cyclic. Then $\phi(\mathcal{C})$ is a $[56, 28, 4]$ self-dual 4- quasi-cyclic code over \mathbb{F}_2 .

Example 4.7 A self-dual cyclic code of length 6 over $R_2 = \mathbb{F}_4 + u\mathbb{F}_4 + v\mathbb{F}_4 + uv\mathbb{F}_4$. The factorisation of $x^6 + 1$ over $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ is given by:

$$x^6 + 1 = (x + 1)^2(x + \alpha)^2(x + \alpha^2)^2.$$

Let \mathcal{C} be the cyclic code over R_2 generated by: $g(x) = e_1g_1(x) + e_2g_2(x) + e_3g_3(x) + e_4g_4(x)$, where $g_1(x) = g_2(x) = \alpha^2 + \alpha^2x + x^2 + x^3$, $g_3(x) = \alpha + \alpha x + x^2 + x^3$ and $g_4(x) = x^3 + 1$. The codes $\mathcal{C}_1 = \mathcal{C}_2 = g_1(x)\mathbb{F}_4[x]$ are $[6, 3, 3]$ self-dual cyclic, $\mathcal{C}_3 = g_3(x)\mathbb{F}_4[x]$ is $[6, 3, 3]$ self-dual cyclic and $\mathcal{C}_4 = g_4(x)\mathbb{F}_4[x]$ is $[6, 3, 2]$ self-dual cyclic. Then $\phi(\mathcal{C})$ is a $[24, 12, 3]$ self-dual 4-quasi-cyclic code over \mathbb{F}_4 .

5 Conclusion

In this paper, the generator polynomials of constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, and their duals are characterized, with help of some decomposition of the ring. We have also given a necessary and sufficient condition on the existence of self-dual constacyclic codes. We have shown that the Gray image of a self-dual cyclic code of length n over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ is a self-dual 4-quasi cyclic code of length $4n$ over \mathbb{F}_{2^m} .

References

- [1] F. W. Anderson and K. R. Fuller, *Rings and categories of modules*, Springer, (1992).
- [2] A. Batoul, K. Guenda and T. A. Gulliver, Constacyclic codes over finite principal ideal rings. Available in <http://arxiv.org/pdf/1505.00876v1.pdf>
- [3] A. R. Calderbank and N. J. A. Sloane, Modular and p-adic codes, *Designs, codes and Cryptography*, 6, (1995), pp. 21-35.
- [4] Y. Cengellenmis, A. Dertli and S. T. Dougherty, Codes over an infinite family of rings with a Gray map, *Designs, Codes and Cryptography*, 72(3), (2014), pp. 559-580.
- [5] M. E. Charkani and J. Kaboré, On Constacyclic codes over \mathbb{Z}_{p^m} , *5th Workshop on Codes, Cryptography and Communication Systems (WCCCS), IEEE*, (2014), pp. 55-58.
- [6] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Transactions on Information Theory*, 50, (2004), pp. 1728-1744.
- [7] S. T. Dougherty, A. Kaya, and E. Saltürk, Cyclic Codes over Local Frobenius Rings of Order 16. Available in <https://dl.dropboxusercontent.com/u/20879623/Cyclic16finalAMC.pdf>.

- [8] K. Guenda and T. A. Gulliver, MDS and self-dual codes over rings. *Finite Fields and Their Applications*, 18(6), (2012), pp. 1061-1075.
- [9] K. Guenda and T. A. Gulliver, Self-dual repeated root cyclic and negacyclic codes over finite fields. *International Symposium on Information Theory Proceedings (ISIT), IEEE*, (2012), pp. 2904 - 2908.
- [10] Y. Jia and S. Ling and C. Xing, On Self-Dual Cyclic Codes Over Finite Fields. *IEEE Transactions on Information Theory* , 57(4), (2011), pp. 2243-2251.
- [11] X. Kai, S. Zhu and Y. Tang, Some constacyclic self-dual codes over integers modulo 2^m , *Finite field and their applications*, 18(2), (2012), pp. 258-270.
- [12] S. Karadeniz, and B. Yildiz, $(1 + v)$ - constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, *Journal of the Franklin Institute*, 348(9), (2011), pp. 2625-2632.
- [13] J. A. Wood, Duality for modules over finite rings and applications to coding theory, *American Journal of Mathematics*, 121(3), (1999), pp. 555-575.
- [14] T. Yao, M. Shi and P. Solé, Skew Cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q^*$. Available in <http://arxiv.org/pdf/1504.07831.pdf>.
- [15] G. Zhang and B. Chen, Constacyclic Codes over $\mathbb{F}_p + v\mathbb{F}_p^*$. Available in <http://arxiv.org/pdf/1301.0669.pdf>.
- [16] S. Zhu, Y. Wang and M. Shi, Some Results on Cyclic Codes Over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Transactions on Information Theory*, 56(4), (2010), pp. 1680-1684.